UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/920,554	08/01/2001	Graeme John Proudler	B-4240 618934-9	4232

22879 7590 07/01/2010

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
07/01/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
laura.m.clark@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte GRAEME JOHN PROUDLER

Appeal 2009-005749
Application 09/920,554
Technology Center 2400

Decided: June 29, 2010

Before KENNETH W. HAIRSTON, JOHN C. MARTIN, and CARLA M. KRIVAK, *Administrative Patent Judges*.

MARTIN, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

This is an appeal under 35 U.S.C. § 134(a) from the Examiner's rejection of claims 1-29 and 31, which are all of the pending claims.

We have jurisdiction under 35 U.S.C. § 6(b). We reverse.

A. Appellant's invention

Appellant's invention relates to a computing platform suitable for performing services, particularly where reliable or trusted performance of some or all of the requested service is required. Specification 1:5-7.[1]

A trusted computing platform is a computing platform into which is incorporated a physical trusted device whose function is to bind the identity of the platform to reliably measured data that provides an integrity metric of the platform (*id.* at 5:1-4). The identity and the integrity metric are compared with expected values provided by a trusted party (TP) that is prepared to vouch for the trustworthiness of the platform (*id.* at 5:4-6). If there is a match, the implication is that at least part of the platform is operating correctly, depending on the scope of the integrity metric (*id.* at 5:6-7).

Figure 6 is reproduced below.

[1] References herein to Appellant's Specification are to the Application as filed rather than to corresponding Patent Application Publication 2002/0023212 A1.

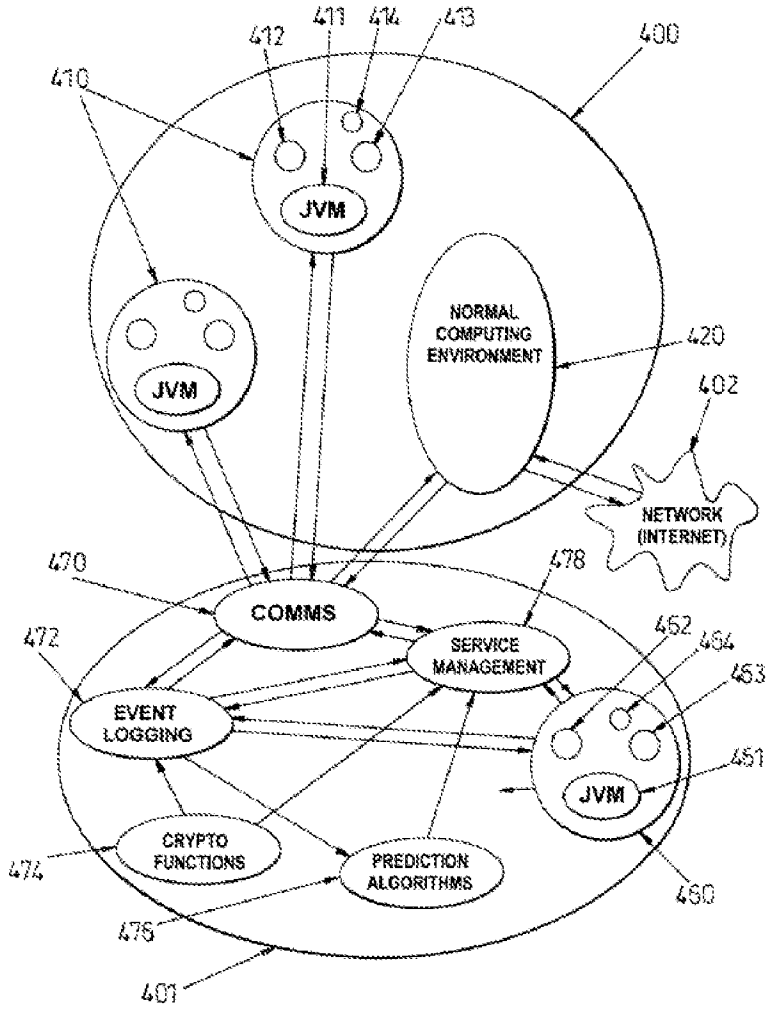

Fig. 6

Figure 6 illustrates schematically the logical architecture of a computing platform in accordance with the invention (*id.* at 14:31-33). This figure shows a logical division between the normal computer platform space 400 (including compartments 410) and the trusted component space 401 (including a trusted compartment 460) (*id.* at 15:1-3, 18-19; 16:10-11).

Figure 8 is reproduced below.

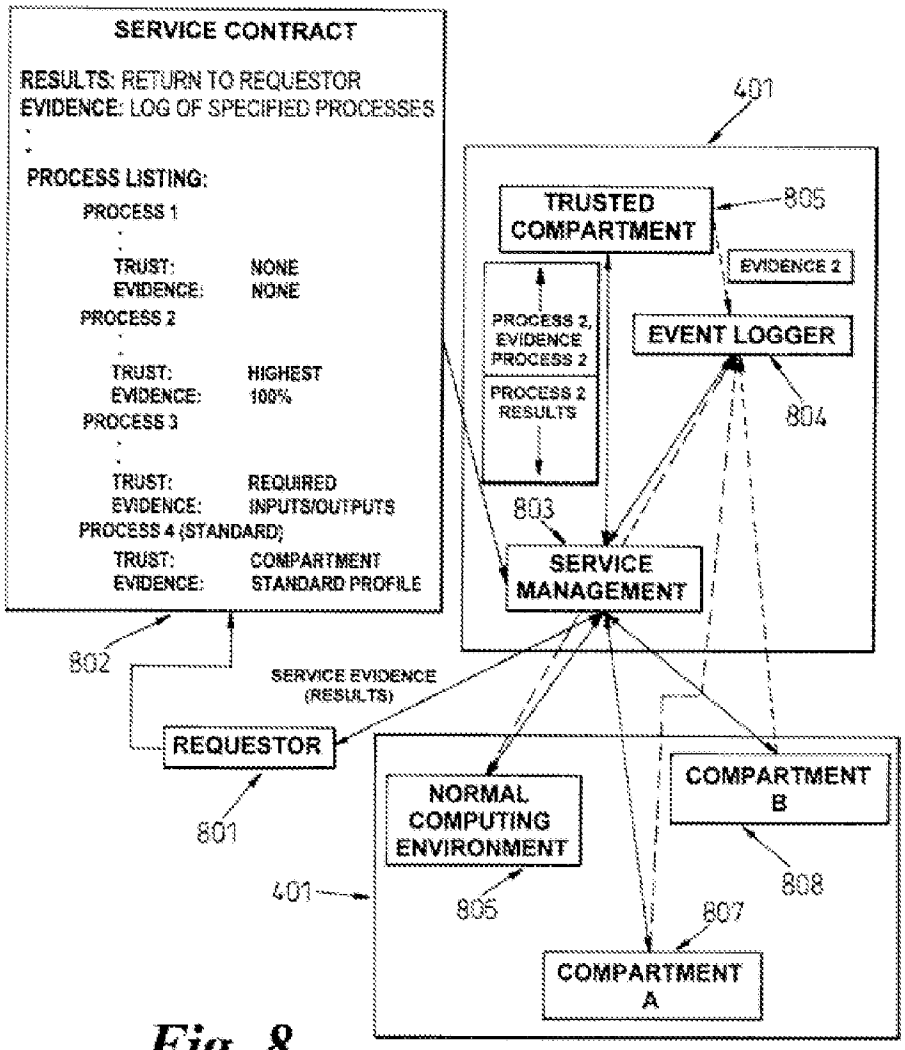

Fig. 8

Figure 8 is a schematic diagram illustrating the performance of a service by the computing platform in accordance with an embodiment of the invention (*id.* at 4:12-13).

A requestor 801 provides a contract 802 to the trusted computing platform 401, where it is received by a service management process 803 (*id.* at 21:32-22:1). The contract specifies where the results are to be provided

(in this case, back to the requestor) and also specifies the level of evidence required--in this case, the evidence is to be provided for the processes in the service for which at least some level of trust is specified (*id.* at 22:1-4).

After the contract is received and accepted, service management process 803 allocates processes in the contract to different computational engines within the trusted computing platform (*id.* at 22:7-10). In the present example, Process 1 does not have any trust requirements and can be allocated to the normal computing environment 806 of the trusted computing platform, whereas Process 2, which requires the "Highest" level of trust, is allocated to trusted compartment 805 (*id.* at 22:12-17). Process 3 has a "Required" level of trust--indicating that trusted performance is required, but at a level below the "Highest" level (*id.* at 22:17-18).

When processes are allocated to the different computing engines, it is also necessary to determine the extent of logging of evidence for each process (*id.* at 22:26-27). In the example depicted in Figure 8, service contract 802 specifies that no logging of evidence is required for Process 1, that 100% logging of evidence is required for Process 2, and that logging of evidence in the form of "inputs and outputs" is required for Process 3 (*id.* at 22:27-23:4).

When compartment 410 (Fig. 6) returns input data to the process, the monitoring process 413 generates, if required, a secure log of the input data (and, advantageously, any associated type tag) (*id.* at 26:10-16).

The service management process 803 (Fig. 8) sends the service results wherever they are required--most typically back to requestor 801 (*id.* at 29:9-10).

B. The claims

The independent claims before us are claims 1 and 24, of which claim 1 reads as follows:

> 1. A method of performing a service for a requestor on a computing platform, comprising:
>
> the requestor providing a specification of the service to be performed to the computing platform, wherein the specification of the service establishes specified levels of trust for at least one of the processes in the service;
>
> the computing platform executing the service according to the specification and logging performance of at least one of the processes for which a level of trust was specified; and
>
> the computing platform providing the requester with a log of the performance of the processes performed according to the specified levels of trust.

Claims App. (Br. 30).

Our understanding of the claim language "wherein the specification of the service establishes specified levels of trust for at least one of the processes in the service" is that the specification identifies a service to be performed and establishes a specified level of trust for at least one process in that service.

C. The references

The Examiner relies on the following references:

McNabb et al. ("McNabb")	US 6,289,462 B1	Sep. 11, 2001
England et al. ("England")	US 6,327,652 B1	Dec. 4, 2001

HP Virtualvault 4.0: Trusted Web-Server Platform. Hewlett Packard Co. (Jan. 1999[2]) [hereinafter *Virtualvault*]

D. The rejections

Claims 1-6, 14-26, 29, and 31 stand rejected under 35 U.S.C. § 103(a) for obviousness over McNabb in view of England. Final Action 7.

Claims 7-13, 27, and 28 stand rejected under 35 U.S.C. § 103(a) for obviousness over McNabb in view of England and Virtualvault. *Id.* at 11.

Appellant specifically argues the merits of only independent claims 1 and 24.

THE ISSUE

The dispositive issue raised by Appellant's arguments[3] is whether the Examiner erred in finding that McNabb and England disclose or suggest a requester that provides, to a computing platform, a specification that identifies a service to be performed and establishes a specified level of trust

---

[2] Answer 2, para. (8).

[3] *See Ex parte Frye*, 94 USPQ2d 1072, 1075 (BPAI 2010) (precedential) ("If an appellant fails to present arguments on a particular issue — or, more broadly, on a particular rejection — the Board will not, as a general matter, unilaterally review those uncontested aspects of the rejection."). Designated as precedential at the following Board website:
(Continued on next page.)

for at least one process in that service.

ANALYSIS

McNabb's invention is a trusted compartmentalized computer operating system. McNabb, title.

In the "Background of the Invention," McNabb explains that an object of the invention is "to provide a secure operating system for use on a firewall or information server where the access is strictly controlled and where the processing is restricted to permit only those actions required to respond to the request" (col. 4, ll. 34-38). Another object is that the authorization of a user requesting data from the system is to be compared to a role established for the user making the request (col. 4, ll. 43-46). McNabb also discloses (col. 7, ll. 28-33) creating an audit trail that enables tracing events forward from the original transactions to related records and reports, and tracing events backward from records and reports to their component source transactions.

McNabb's system employs a sensitivity label (SL) that represents the security level of a request and describes the sensitivity (e.g., classification) of the data in the object (col. 8, ll. 33-36). Figure 2 shows extended attributes (including a sensitivity label 202) applied to files, while Figure 3 shows attributes (including maximum and minimum sensitivity labels 254

---

http://www.uspto.gov/ip/boards/bpai/decisions/prec/index.jsp.

and 256) applied to the processes and the packets that are processed on the system (col. 9, ll. 10-13; col. 10, ll. 12-13).

McNabb explains that a control method may be applied to a software application suite, wherein each user is permitted to operate upon or view data at the user's sensitivity level (col. 19, ll. 59-62). This may, for instance, allow a commercial software product to be executed such that a hierarchical security system may be applied externally to the software application suite, where each user that executes the software would be supplied with a customized or personalized version (col. 19, ll. 62-67). The Examiner reads the claim language "requestor providing a specification of the service to be performed to the computing platform" (claim 1) on a user's request to run such commercial software on McNabb's trusted computer system. *See* Final Action 7, para. 7 ("McNabb discloses a method including a requester providing a specification of a service to be performed that establishes required sensitivity levels for processes in the service (see, for example, column 19, line 55-column 20, line 2, where different processes are specified for different sensitivity levels).").

The Examiner agrees with Appellant that the "levels of trust" recited in claim 1 do not read on the sensitivity levels (SLs) of the user requests in McNabb. Specifically, at page 2 of the December 12, 2005, non-final Office Action, the Examiner was persuaded to withdraw a rejection of claim 1 for anticipation by McNabb by arguments at pages 2-4 of Appellant's "Response to Final," filed November 8, 2005. In page 2 of that Response, Appellant argued that

> the "security level" [in McNabb] has to do with whether or not the user can be trusted. For example, security level asks the question "does the user have a sufficiently high security level on the computer to perform certain actions"? The level of trust works in the opposite direction. Can a user, whatever their security level might be, trust the computer that they are using to reliability [sic] "process sensitive or classified information without fear of denial of service, data theft, or corruption resulting from hostile activity" as mentioned in McNabb? That has nothing to do with their access privileges (their security level).

As a result, in the Final Action under review in this appeal proceeding, the Examiner finds that "McNabb does not explicitly disclose details of establishing the trust in the computer system, nor does McNabb explicitly disclose levels of trust" (Final Action 9-10) and relies on England for such a teaching (*id.*).

England's invention bears little resemblance to McNabb's invention. England addresses "a need in the art for guaranteeing that a digital rights management operating system [DRMOS] has been properly loaded on a computer" and is "readily discernable from a non-trusted operating system executing on the same computer." England, col. 3, ll. 56-61. England guarantees proper loading of the DRMOS on a subscriber computer by validating the digital signature for each component to be loaded and determining a trust level for each component (col. 4, ll. 5-8). The digital rights management operating system is deemed to have a trusted identity only if components having valid signatures and a predetermined trust level have been loaded; otherwise, the operating system is considered to have an untrusted identity (col. 4, ll. 8-12).

The Examiner finds that "England . . . discloses a requester providing a specification of a service to be performed that establishes required trust levels for processes in the service (column 9, lines 42-51; column 19, lines 13-40)" (Final Action 8). The cited lines in column 9 describe the messages that are exchanged when an application 209 in a subscriber computer 200 (Fig. 2) issues a request to download of content from a content provider 220. Specifically, DRMOS 205 in subscriber computer 200 sends a message 3 to the provider 220 requesting content 221 (col. 9. ll. 43-44). The content provider responds by transmitting a challenge message 4 to the DRMOS asking for the identity of the CPU 201, the DRMOS, and the application 209 (col. 9, ll. 44-48). DRMOS 205 then issues a response message 5 containing a certificate 202 for the CPU 201, the DRMOS's identity 206, and the rights manager certificate 210 for application 209 (col. 9, ll. 48-51). The cited lines of column 19 explain that in order to protect downloaded content from unauthorized access, the content provider attaches an access predicate that can also include a license to the content (col. 19, ll. 6-10). The access predicate can take the form of a "required properties" access control list (ACL) 1000 (Fig. 10) that contains a basic trust level field 1001 specifying the minimum rights management functions that must be provided by any application wishing to process the content (col. 19, ll. 13-18). These minimum functions can be established by a trade association, such as the MPAA (Motion Picture Association of America), or by the DRMOS vendor (col. 19, ll. 18-21). ACL 1000 can also include one or more extended trust level fields 1003 containing identifiers that specify additional rights

management functions that must be provided by the subscriber computer, such as requiring that only a certain version of a particular application be allowed access to the content (col. 19, ll. 25-31). The DRMOS is responsible for checking the "required properties" ACL and for enforcing the licensing restrictions (col. 20, ll. 14-16).

Regarding the first paragraph of claim 1 (calling for a requestor to provide, to a computing platform, a specification that identifies a service to be performed and establishes a specified level of trust for at least one process in that service), the Examiner concluded that

> it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of McNabb to incorporate levels of trust as taught by England, in order to guarantee the ability to distinguish between trusted and non-trusted systems executing on the same computer (see England, column 3, lines 56-61).

Final Action 8.[4] We agree with Appellant that the manner in which the Examiner is proposing to combine the reference teachings is not clear from the discussion of the rejection. *See* Br. 11 ("Exactly what elements disclosed in McNabb are supposed to be combined with exactly what elements in England . . .?").

Appellant assumes that the Examiner is "tr[ying] to substitute McNabb's sensitivity levels for England's trust levels" (Br. 12) and properly asks: "Why do that, especially considering that fact that they are not the

[4] The second and third paragraphs of claim 1, which are directed to the logging feature, are addressed separately *infra*.

same thing? The trust levels in England have to do with convincing a content provider to make digital content available, and not with the content provider trying to run some service on McNabb's [sic; England's] computer!" (*Id.*). Appellant further argues that assuming for the sake of argument that the reference teachings can be combined, McNabb and England are directed solely to servers and client computers, respectively, and that therefore the only reasonable combination of the reference teachings would be a system that includes a client computer like England's and a server like McNabb's, a combination Appellant contends will not satisfy at least the first paragraph of claim 1 (Br. 15-18).

The Examiner (Answer 11-12) disputes Appellant's characterization of McNabb and England as directed solely to servers and client computers, respectively, which suggests to us that the Examiner is not proposing a system that includes a client computer like England's and a server like McNabb's. However, the Examiner has not adequately explained *how* to "modify the method of McNabb to incorporate levels of trust as taught by England, in order to guarantee the ability to distinguish between trusted and non-trusted systems executing on the same computer" (Final Action 8). As support for combining the reference teachings, the Examiner has stated that "because both the McNabb and England references are directed to secure and/or trusted operating systems, and are therefore analogous art, there would be a reasonable expectation that one would be successful in combining features from the two systems" (Answer 9). Although a finding that a reference constitutes analogous art can be strong evidence of obviousness, it is not

necessarily dispositive. *See In re ICON Health & Fitness, Inc.*, 496 F.3d 1374, 1380 (Fed. Cir. 2007) ("while perhaps not dispositive of the issue, the finding that Teague, by addressing a similar problem, provides analogous art to Icon's application goes a long way towards demonstrating a reason to combine the two references."). The *ICON Health & Fitness* court then went on to analyze the arguments for and against combining the teachings of the references. *Id.* at 1380-81.

We are therefore reversing the rejection of claim 1 because the Examiner has not provided the necessary "*articulated reasoning* with some rational underpinning to support the legal conclusion of obviousness." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (emphasis added).[5]

For the same reason, we are reversing the rejection of independent claim 24 and the rejections of dependent claims 2-23, 25-29, and 31.

DECISION

The rejections of claims 1-29 and 31 under 35 U.S.C. § 103(a) for obviousness over the prior art are reversed.

REVERSED

[5] We therefore do not reach the question of whether the combined reference teachings satisfy the second and third paragraphs of claim 1, which relate to logging.

gvw

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
P. O. Box 272400
Mail Stop 35
FORT COLLINS, CO 80528